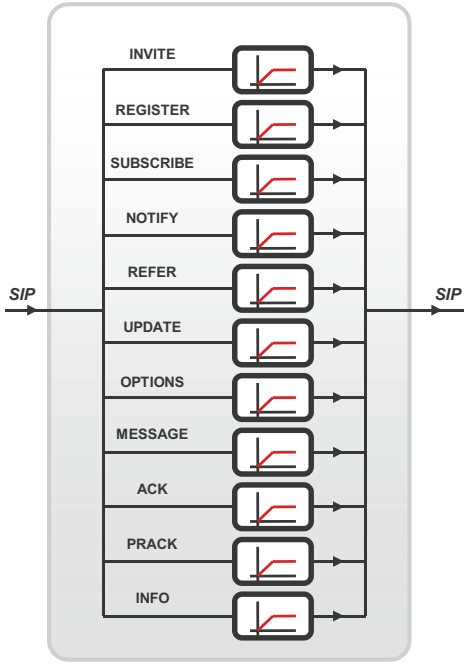
Voice over IP (VoIP) Protection

Protection for Voice over IP (SIP and SDP) services in Unified Communication and NGN/IMS networks with FortiOS.

Advanced Voice over IP Protection

The FortiOS SIP Application Level Gateway (ALG) provides the following advanced VoIP defense mechanisms:

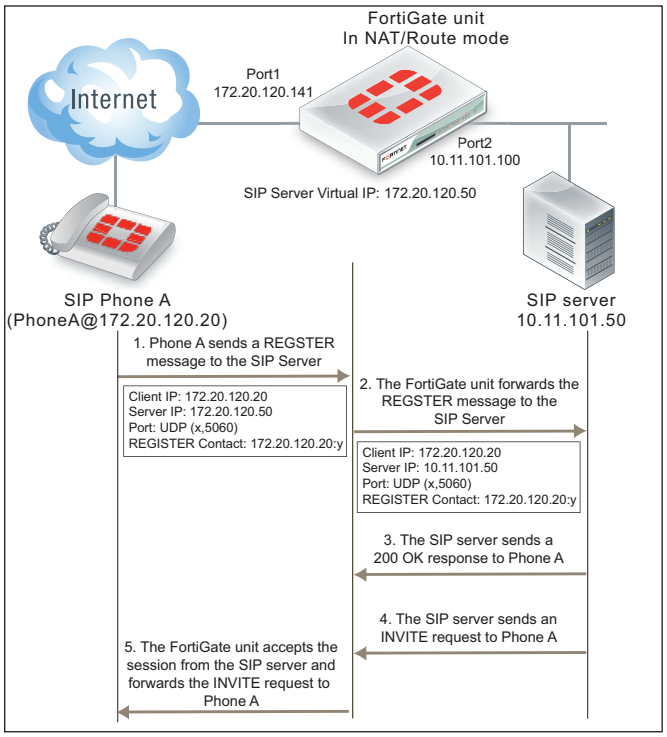
- **Deep SIP message inspection (also called deep SIP header inspection):** Verifies SIP and SDP header syntax and protects SIP servers from potential SIP Fuzzing attacks. When a violation is detected, FortiOS can impose counter measures and can also send automatic SIP response messages to offload processing from the SIP server.
- **SIP message rate limiting:** Allows rate limiting of SIP messages per SIP request method. This prevents a SIP server from overload or from DoS attacks with particular SIP methods. For example, FortiOS can protect SIP servers from a flood of SIP REGISTER or INVITE messages, which can be caused by a DoS attack or a flash crowd.
- **RTP and RTCP pinholing:** RTP pinholing only forwards RTP/RTCP packets that conform to the particular session description of the associated SIP dialog. If a SIP dialog is finished, FortiOS automatically closes the pinhole. RTP/RTCP pinholing is supported by FortiASIC acceleration and achieves high packet throughput at low jitter and delay.
- **Stateful SIP dialog tracking:** FortiOS tracks SIP message sequences and prevents unwanted SIP messages that are not related to a particular SIP dialog. For instance, FortiOS can detect malicious SIP BYE messages that do not conform with the associated context of the SIP dialog.
- **Inspecting SIP over SSL/TLS (secure SIP):** Some SIP phones and SIP servers use SSL or TLS to encrypt SIP signalling traffic. To allow SIP over SSL/TLS calls to pass through the FortiGate unit, the encrypted signalling traffic has to be unencrypted and inspected. FortiOS intercepts and unencrypts and inspects the SIP packets. Allowed packets are then re-encrypted and forwarded to their destination.



- **Inspecting SIP on multiple ports:** FortiOS can detect and inspect SIP and SDP traffic received on two configurable ports. The port configuration can be changed without affecting other parts of the SIP configuration.

Carrier Grade

To protect VoIP infrastructure in carrier networks, FortiOS complies with typical carrier requirements for availability and robustness.

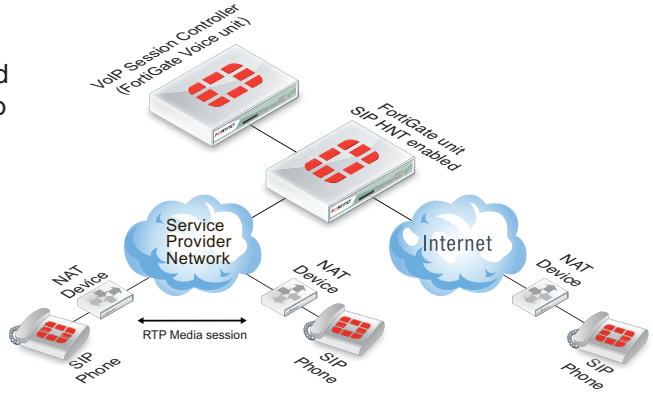


- **High Availability:** FortiOS supports a hot failover configuration with an active and a standby FortiGate device. FortiOS dynamically updates the context on the standby unit with SIP and RTP related data. This enables the standby unit to takeover stable voice calls in case of a planned or unplanned outage or failover of the active unit.
- **Geographical Redundancy of SIP servers:** In FortiOS SIP server cluster configurations the active and standby units can be deployed in different geographical locations. This configuration prevents a total outage of a SIP server infrastructure if one location goes offline. FortiOS supports the detection of SIP server outages (loss of heartbeats) and a redirect of SIP messages to the redundant SIP server location.
- **Logging and Reporting:** FortiOS can log call related information internally or to an external SYSLOG or FortiAnalyzer unit. This includes event logs that show particular SIP-related attacks or syntax violations with SIP messages or logs that summarize call statistics.

Header Manipulation

FortiOS SIP and SDP header manipulation supports SIP Network Address Translation (NAT) through FortiGate units configured as NAT firewalls.

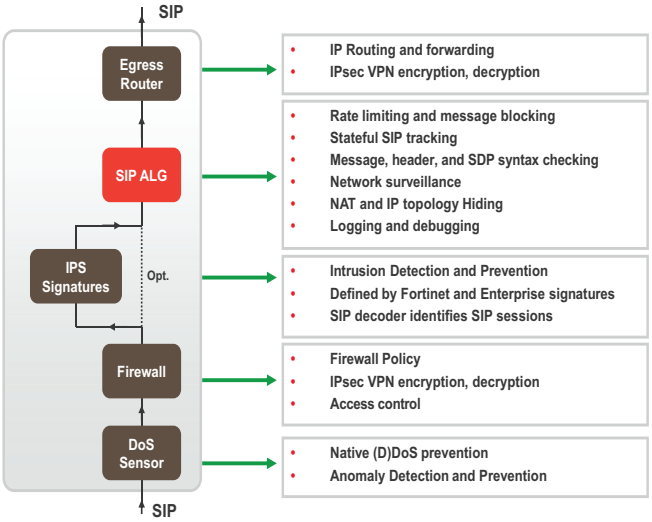
- **NAT/NAPT:** FortiOS performs configurable network address translation for IP addresses in the SIP and SDP header. The SIP ALG follows the configured NAT addresses in firewall virtual IPs and changes SIP header IP addresses accordingly. RTP NAT is controlled by SIP/SDP and the firewall policy. This allows translating an unlimited number of IP addresses without adding specific RTP policies.
- **Hosted NAT traversal (HNT):** In many service provider networks, CPE firewall devices provide NAT without application awareness. This causes issues for SIP/SDP and RTP traffic, since UAC IP address information references to the internal network behind the far end firewall. VoIP calls cannot be connected successfully. FortiOS mitigates far end NAT issues (called Hosted NAT traversal) by probing the first RTP packet from the UAC and learning the far end NA(P)T binding. FortiOS then updates the internal NAT binding for RTP accordingly.



- **IP Address conservation for NAT:** In case of SIP and RTP NAT IP the original address information can get lost after translating to the provisioned IP addresses. This IP address information is sometimes required for detailed billing records or debugging purposes. FortiOS can maintain the original IP address information in a translated SIP header by adding it to the SIP/SDP info line (i=) or by adding it to the original attribute (o=). Either option can be selected depending on the SIP billing environment.

SIP ALG activation

The FortiOS SIP ALG is applied to SIP traffic accepted by a firewall policy that includes a VoIP profile. The VoIP profile controls how the SIP ALG processes SIP sessions. FortiOS also includes a high-performance SIP session helper that provides limited SIP functionality. In most cases the SIP ALG should be used because the SIP ALG supports the complete range of FortiOS SIP features.



SIP over IPv6

FortiOS, operating in NAT/Route and in Transparent mode supports SIP over IPv6. The SIP ALG can process SIP messages that use IPv6 addresses in the headers, bodies, and in the transport stack. The SIP ALG cannot modify the IPv6 addresses in the SIP headers so FortiGate units cannot perform SIP or RTP NAT over IPv6 and also cannot translate between IPv6 and IPv4 addresses.

Platform support and hardware acceleration

FortiOS supports VoIP protection with the SIP ALG on all FortiGate hardware platforms. Whenever a FortiGate unit provides FortiASIC or SPM HW acceleration, the SIP ALG will use this option to fast-path RTP/RTCP traffic. This provides a high throughput solution at very low jitter and delay. FortiOS provides efficient and highly scalable protection for VoIP in emerging Enterprise and Carrier network. This complements Fortinet's UTM offering. VoIP protection can be easily added as VoIP profile to any firewall policy.

VoIP protection is supported in FortiAnalyzer and FortiManager. Centralized logging and management are essential for carrier and MSSP service provider and are influencing business case calculations.